AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A gateway device disposed between a data center and a network for thwarting denial of service attacks on the data center, the gateway device ~~comprises~~ comprising:

a computing device ~~comprising~~ that performs:

a monitoring process that monitors network traffic through the gateway device;

a communication process that communicates statistics collected in the gateway from the monitoring process with a control center and that receives queries or instructions from the control center; and

a filtering process to insert filters on network devices to filter out packets that the gateway deems to be part of an attack.

2. (Original) The gateway of claim 1 wherein the communication process couples to a dedicated link to communicate with the control center over a hardened network.

3. (Original) The gateway of claim 1 wherein the monitoring process in the gateway samples network packet flow in the network.

4. (Original) The gateway of claim 1 wherein the gateway is adaptable to be physically deployed in line in the network.

5. (Original) The gateway of claim 1 wherein, the gateway is adaptable to dynamically install the filters on nearby routers.

6. (Original) The gateway of claim 1 wherein the monitoring process detects IP traffic and determines levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

7. (Original) The gateway of claim 1 wherein the monitoring process detects Internet Protocol (IP) traffic and determines levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addersses.

8. (Currently amended) The gateway of claim 1 wherein the monitoring process detects Internet Protocol (IP) traffic and determines levels of Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) packets to unused ports.

9. (Currently amended) The gateway of claim 1 wherein the monitoring process detects IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

10. (Currently amended) The gateway of claim 1 wherein the monitoring process detects sustained rate higher than plausible for a human user over a persistent HTTP connection.

11. (Currently amended) The gateway of claim 1 wherein the monitoring process maintains statistical summary information of traffic over different periods of time and at different levels of detail.

12. (Currently amended) The gateway of claim 11 wherein the monitoring process maintains statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

13. (Currently amended) The gateway of claim 12 wherein the monitoring process has configurable thresholds and issues a warning when one of the measured parameters exceeds the corresponding threshold.

14. (Currently amended) The gateway of claim 13 wherein the monitoring process logs packets.

15. (Currently amended) The gateway of claim 14 wherein the monitoring process logs specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

16. (Currently amended) A method of protecting a victim site during a denial of service attack, ~~comprises~~ comprising:

disposing a gateway device between the victim site and a network;

monitoring network traffic through the gateway device and measuring heuristics of the network traffic to provide statistics network traffic;

communicating the statistics collected in the gateway device to a control center; and

filtering out packets that the gateway or control center deems to be part of an attack.

17. (Currently amended) The method of claim 16 wherein the communicating process occurs over a dedicated link to the control center via a hardened network.

18. (Currently amended) The method of claim 16 wherein the monitoring process samples network packet flow in the network.

19. (Original) The method of claim 16 wherein the gateway is physically deployed in line in the network.

20. (Currently amended) The method of claim 16 wherein the filtering process further comprises:

dynamically installing filters on nearby routers via an out of band connection.

21. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

detecting IP traffic and determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

22. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

detecting Internet Protocol (IP) traffic and determining levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

23. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

detecting Internet Protocol (IP) traffic and determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

24. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

detecting IP traffic and determines levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

25. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

26. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

logging statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

27. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

28. (Currently amended) The method of claim 16 wherein the monitoring process further comprises:

logging specific packets identified as part of an attack to enable an administrator to identify important properties of the attack.

29. (Currently amended) A computer program product residing on a non-transitory computer readable storage medium ~~for protecting a victim site during a denial of service attack~~, ~~comprises~~ storing instructions that when executed by a computer cause the computer to perform a method for ~~causing a computer device coupled at an entry to the site to~~ protecting a victim site during a denial of service attack, the method comprising:

~~monitor~~ monitoring network traffic sent to the victim site and ~~measure~~ measuring heuristics of the network traffic to provide statistics on the network traffic;

~~communicate~~ communicating the statistics collected in the computer device to a control center; and

~~filter~~ filtering out packets that the device or control center deems to be part of an attack.

30. (Currently amended) The computer program product of claim 29, wherein the monitoring process further comprises sampling network flow~~instructions to monitor further comprise instructions to:~~

~~sample network traffic flow~~.

31. (Currently amended) The computer program product of claim 29, ~~wherein instructions to filter further comprise instructions to:~~the filtering process further comprising:

dynamically ~~install~~ installing filters on nearby routers via an out of band connection.

32. (Currently amended) The computer program product of claim 29, ~~wherein instructions to monitor further comprise instructions to~~ the monitoring process further comprising:

~~detect~~ detecting IP traffic; and

~~determine~~ determining levels of unusual amounts of IP fragmentation or fragmented IP packets with bad or overlapping fragment offsets.

33. (Currently amended) The computer program product of claim 29, ~~wherein instructions to monitor further comprise instructions to~~ the monitoring process further comprising :

~~detect~~ detecting Internet Protocol (IP) traffic; and

~~determine~~ determiing levels of IP packets that have bad source addresses or Internet Control Message Protocol (ICMP) packets with broadcast destination addresses.

34. (Currently amended) The computer program product of claim 29, ~~wherein instructions to monitor further comprise instructions to~~ the monitoring process further comprising:

~~detect~~ detecting Internet Protocol (IP) traffic; and

~~determine~~ determining levels of Transport Control Protocol (TCP) or User Datagram Protocol UDP packets to unused ports.

35. (Currently amended) The computer program product of claim 29, ~~wherein instructions to monitor further comprises instructions to~~ the monitoring process further comprising:

~~detect~~ detecting IP traffic; and

~~determine~~ determining levels of TCP segments advertising unusually small window sizes, which may indicate a load on the data center, or TCP ACK packets not belonging to a known connection.

36. (Currently amended) The computer program product of claim 29, ~~wherein instructions to monitor further comprises instructions to~~ the monitoring process further comprising:

~~detect~~ detecting a sustained rate of reload requests that is higher than plausible for a human user over a persistent HTTP connection.

37. (Currently amended) The computer program product of claim 29, ~~wherein instructions to monitor further comprises instructions to~~ the monitoring process further comprising:

~~log~~ logging statistics on parameters including source and destination host or network addresses, protocols, types of packets, number of open connections or of packets sent in either direction.

38. (Currently amended) The computer program product of claim 29, ~~wherein instructions to monitor further comprises instructions to~~ the monitoring process further comprising:

~~issue~~ issuing a warning to the control center when one of the measured parameters exceeds a corresponding configurable threshold.

39. (Currently amended) The computer program of claim 29, ~~further comprising instructions to cause the processor to receive~~ the communicating process further comprising receiving communications from ~~a~~ the control center to deliver data pertaining to the types of traffic passing through the gateway.